DIRECTOR
OF
CENTRAL
INTELLIGENCE

DCI Security Committee

Minimum Standards For Security Awareness Programs In The U.S. Intelligence Community

SECOM-D-543
July 1979

Minimum Standards For Security Awareness Programs In The U.S. Intelligence Community

Minimum standards are hereby established for the security education programs designed to enhance the security awareness of U.S. Government employees and private contractors working in the U.S. Intelligence Community. Compliance with these standards is required for all Departments/Agencies within the Intelligence Community. It is intended that existing security awareness programs shall be modified to conform with these standards. Departments/Agencies will establish a documented program, to ensure that training has been presented to all personnel.

The security awareness requirements set forth herein are divided into three phases. Phase I concerns the initial indoctrination of the employee which is normally administered prior to access to classified information. Phase II concerns the continuing security awareness program required to maintain and increase security awareness throughout the period of access. Phase III sets forth the final guidelines and instructions when access to classified information is terminated.

I. Initial Indoctrination—As soon as practicable after being approved for access to classified information, employees shall receive an initial security indoctrination which shall include:

A. The need for and purpose of classified information, and the adverse effects to the national security that could result from unauthorized disclosure.

B. The intelligence mission of the Department/Agency to include the reasons why intelligence information is sensitive.

C. The administrative, personnel, physical and other procedural security requirements of the Department/Agency, and those requirements peculiar to specific duty assignments.

D. Individual classification management responsibilities as set forth in appropriate directives and regulations to include classification/declassification guidelines and marking requirements.

E. The definitions and criminal penalities for espionage, including harboring or concealing persons; gathering, transmitting, or losing defense information; gathering or delivering defense information to aid foreign governments; photographing and sketching defense installations; unauthorized disclosure of classified information (Title 18, U.S.C., Sections 792 through 795, 797 and 798), the Internal Security Act of 1950 (Title 50, U.S.C., Section 783) and, when appropriate, the Atomic Energy Act, Sections 224 through 227.

F. The administrative sanctions for violation or disregard of security procedures.

G. A review of the techniques employed by foreign intelligence organizations in attempting to obtain national security information.

H. Individual security responsibilities including:

1. The prohibition against discussing classified information in a nonsecure area, over a nonsecure telephone or in any other manner that permits access by unauthorized persons.

2. The need to determine, prior to disseminating classified information, that the prospective recipient has the proper security clearance, that the classified information is needed in order to perform official duties and that the recipient can properly protect the information.

3. Administrative reporting requirements such as foreign travel, contacts with foreign nationals, attempts by unauthorized individuals to obtain national security information, physical security deficiencies and loss or possible compromise of classified material.

4. Obligation to report to proper authorities any information which could reflect on the trustworthiness of an individual who has access to classified information, such as:

a. Willful violation of security regulations

b. Unexplained affluence or excessive indebtedness

c. Serious unlawful acts

d. Apparent mental or emotional problems

e. Coercion or harassment attempts

f. Blackmail attempts

5. Identification of the elements in the Department/Agency to which matters of security interest are to be referred.

II. Periodic Employee Awareness Enhancement—Each Department/Agency shall establish a continuing security awareness program which will provide for frequent exposure of personnel to viable security awareness material. Implementation of a continuing program may include live briefings, audio-visual presentations (e.g., video tapes, films and slide/tape programs), printed material (e.g., posters, memoranda, pamphlets, fliers) or a combination thereof. It is essential that current information and materials are utilized. Programs should be designed to meet the individual needs of the Department/Agency.

A. The basic elements for this program shall include, but are not limited to, the following:

1. The foreign intelligence threat.

2. The technical threat.

3. Administrative, personnel, physical and procedural security.

4. Individual classification management responsibility.

5. Criminal penalties and administrative sanctions.

6. Individual security responsibilities.

7. A review of other appropriate Department/Agency requirements.

B. Special security briefings/debriefings are required to supplement the existing security awareness programs in the following situations:

1. When an employee is designated as a courier.

2. When an employee travels, officially or unofficially, to or through communist countries, or areas of high risk.

3. When an employee has, or anticipates, contact with representatives of communist controlled countries.

4. When an employee is granted access to sensitive compartmented information or crytographic material.

5. When any other situation arises for which a special briefing/debriefing is required by the Department/Agency.

III. Debriefing—When a Department/Agency has determined that access to classified information is no longer required, final instructions and guidelines will be provided to the employee. As a minimum these shall include:

A. A requirement that the individual read appropriate section of Titles 18 and 50, U.S. Code and that the intent and criminal sanctions of these laws relative to espionage and unauthorized disclosure be clarified.

B. The continuing obligation never to divulge, publish, or reveal by writing, word, conduct or otherwise, to any unauthorized persons any classified information relating to the national security, without the written consent of appropriate Department/Agency officials.

C. An acknowledgement that the individual will report without delay to the Federal Bureau of Investigation, or the Department/Agency, any attempt by an unauthorized person to solicit national security information.

D. A declaration that the individual no longer possesses any documents or material containing classified information.

E. A reminder of the risks associated with foreign travel and certain hazardous activities as defined in DCID 1/20, and Department/Agency reporting requirements as applicable.